

# LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS

DOCUMENTATIE

INTREABA PROFESORUL

CURSURILE MELE

9 NETFILTER » 9.3 Structura NETFILTER » 9.3.3 The state machine

■ 1. Shell Scripts
■ 2. Linux Kernel
■ 3. Serverul DHCP
■ 4. Serverul FTP
■ 5. NFS - Network File System
■ 6. Serverul DNS
■ 7. Serverul Apache
■ 8. Serverul MySQL
■ 9. NETFILTER
■ 9.1 Prezentare generala
■ 9.2 Firewall
■ 9.3 Structura NETFILTER
■ 9.3.1 Chains
■ 9.3.2 Tables
■ 9.3.3 The state machine
■ 9.4 Sintaxa iptables
■ 9.5 Scenarii si exemple
■ 10. Sistemul de e-Mail
■ 11. Serverul Postfix
■ 12. Serverul POP/IMAP
■ 13. Managementul Logurilor
■ 14. Exemple practice (Ubuntu 14.04 LTS)
■ 15. Webmin

## The state machine

Connection tracking este componenta NETFILTER care ofera acestuia statutul de firewall stateful. Aceasta poate lua decizii de filtrare a pachetelor nu in functie de headerul Layer3 (IP) si Layer4 (TCP/UDP) ci in functie de relatia pachetului cu celelalte pachete.

Connection tracking este realizat de un framework din kernel care se numeste **conntrack**. Aceasta poate fi incarcat ca modul sau poate fi parte integranta a kernelului.

conntrack reprezinta o parte din NETFILTER care identifica pachetele ca aflandu-se intr-o anume stare in functie de relatia cu celelalte pachete din acelasi stream.

NETFILTER defineste 4 stari pentru fiecare pachet:

### 1. NEW

Primul pachet dintr-o conexiune generata de hostul local se gaseste in starea **NEW**.

### 2. ESTABLISHED

Pachetul destinat hostului local ca raspuns la pachetul trimis anterior isi schimba starea in **ESTABLISHED** in momentul in care intra in **PREROUTING**. Sunt toate pachetele dintr-o conexiune mai putin primul care a initiat conexiunea si care se afla in starea NEW.

### 3. RELATED

In starea **RELATED** se gasesc acele pachete legate de un alt flux de date

**Exemplu:** in cazul FTP activ, conexiunea de date de pe portul 20 ca raspuns la conexiunea de control initiatata catre portul 21

### 4. INVALID

Sunt acele pachete ale caror header contine informatii neconcordante.

**Exemplu:** un pachet al carui header TCP contine atat flag-ul **syn** cat si **fin**

Informatiile pe care modulul conntrack le foloseste pentru a sti in ce stare se gaseste un pachet, pot fi vizualizate in **/proc/net/nf\_conntrack**

```
tcp 6 117 SYN_SENT src=192.168.1.6 dst=192.168.1.9 sport=32775 \
dport=22 [UNREPLIED] src=192.168.1.9 dst=192.168.1.6 sport=22 \
dport=32775 [ASSURED] use=2
```

Detalii:

tcp - protocolul de transport;

6 - valoarea campului protocolului din headerul IP;

117 - nr. de secunde in care aceasta intrare este valida. Timpul este decrementat continuu pana cand apare trafic legat de aceasta conexiune. Apoi timpul este resetat cu valoarea default;

SYN\_SENT - trafic doar intr-o directie;

src - ip source;

dst - ip destinatie;

sport - port sursa;

dport - port destinatie;

UNREPLIED - nu a existat trafic in ambele directii. In momentul in care apare trafic in ambele directii UNREPLIED se inlocueste cu ASSURED;

ASSURED (la final) - informatii despre aceasta conexiune nu vor fi sterse cand se atinge nr. maxim de conexiuni;

## Nota



La anumite versiuni fisierelor referitoare la NETFILTER apar doar dupa ce se foloseste conntrack machine adica dupa ce se incarca in memorie firewall-ul ce contine regulile cu referire la starile unui pachet.

## Resurse

- Connection tracking

© 2006-2016 Crystal Mind Academy. All rights reserved